भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

RBI/2022-23/xx
DoS.CO.CSITEG/SEC.xx/31.01.015/2022-23 October 20, 2022

The Chairman/Managing Director/Chief Executive Officer

Scheduled Commercial Banks (excluding Regional Rural Banks);
Small Finance Banks;
Payments Banks;
Non-Banking Financial Companies in Top, Upper and Middle Layers;
All India Financial Institutions (NHB, NABARD, SIDBI, EXIM Bank and NaBFID); and
Credit Information Companies.

Madam/Dear Sir,

Draft Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices

Please refer to para IV (8) of the Statement on Developmental and Regulatory Policies released with the Bi-monthly Monetary Policy Statement 2021-22 on February 10, 2022, wherein it was announced that draft guidelines, updating and consolidating the instructions relating to Information Technology (IT) Governance and Controls, Business Continuity Management and Information Systems Audit, will be issued by the Reserve Bank of India.

2. Accordingly, the Reserve Bank proposes to prescribe a Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, to be implemented by the Regulated Entities (REs) as given in the **Annex**.

Yours faithfully,

(T.K.Rajan)
Chief General Manager

Encl: Annex

Annex

Draft Master Direction – Information Technology Governance, Risk, Controls and Assurance Practices

In exercise of the powers conferred by Section 35A of the Banking Regulation Act, 1949; Section 45L of the Reserve Bank of India Act, 1934 and Section 11 of the Credit Information Companies (Regulation) Act, 2005, and all other provisions/ laws enabling the Reserve Bank of India in this regard, the Reserve Bank being satisfied that it is necessary and expedient in the public interest to do so, hereby issues the Directions hereinafter specified.

CHAPTER – I

Preliminary

1. Short Title and Commencement
   a. These Directions shall be called the Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2022.
   b. These Directions incorporate consolidated and updated guidelines/ instructions/ circulars on IT Governance, Risk, Controls, Assurance Practices and Business Continuity/ Disaster Recovery Management. The list of circulars consolidated is given in Chapter VII of this Master Direction.
2. These Directions shall come into effect six months from the date of issue, i.e., date on which the final Master Direction is placed on the official website of the Reserve Bank of India (RBI).

3. Applicability

These Directions shall apply to the following Regulated Entities (REs) unless explicitly exempted:

   a. Scheduled Commercial Banks (excluding Regional Rural Banks);
   b. Small Finance Banks;
   c. Payments Banks;
   d. All Non-Banking Financial Companies (NBFCs) in Top, Upper and Middle Layers as per Scale Based Regulation (SBR)[1];

[1] Ref: RBI/2021-22/112 DOR.CRE.REC.No.60/03.10.001/2021-22 circular on Scale Based Regulation (SBR): A Revised Regulatory Framework for NBFCs dated October 22, 2021.

e. All India Financial Institutions (NHB, NABARD, EXIM Bank SIDBI and NaBFID); and
f. Credit Information Companies.

4. Definitions

All expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949 or the Reserve Bank of India Act, 1934 or Credit Information Companies (Regulation) Act, 2005 or Information Technology Act, 2000 or Companies Act, 2013 and Rules made thereunder or any statutory modification or re-enactment thereto or as used in RBI Directions / Circulars, as the case may be.

CHAPTER – II
IT Governance

5. REs shall put in place a robust IT Governance Framework comprising of governance structure and processes necessary to meet the RE's business/ strategic objectives. The governance framework shall specify the role (including authority) and responsibilities of the Board of Directors (Board) / Board level Committee/ Local Management Committee (in case of foreign banks operating as branches in India)[2] and Senior Management. The Framework must, *inter alia*, include adequate oversight mechanisms to ensure accountability and mitigation of business risks. The key focus areas of IT Governance shall include strategic alignment, value delivery, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management.
6. Strategies, Policies related to IT, Information Systems (IS), Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management) shall be approved by the Board and reviewed at least annually. Enterprise-wide risk management policy or operational risk management policy needs to incorporate IT-related risks also.

IT Strategy Committee

7. REs shall establish a Board-level IT Strategy Committee (ITSC) with a minimum of two directors[3] as members. At least one member should have substantial expertise in managing/ guiding technology initiatives. The IT Strategy Committee shall meet at least on quarterly basis.

8. The Board/ IT Strategy Committee shall, *inter alia*:
   a) Ensure that the RE has put an effective IT strategic planning process in place;

[2] For foreign banks operating as branches in India, any reference to Board/ Board level Committees in this Master Direction shall be interpreted as Local Management Committee or an equivalent Committee. The CEO of Indian operations shall be responsible for effective oversight of IT Governance, risk, controls, as well as statutory and regulatory compliance in respect of all operations in India.

[3] For foreign banks operating as branches in India, minimum of two members of the Local Management Committee or an equivalent Committee shall be the members of IT Strategy Committee.

b) Guide in preparation of IT Strategy, containing over-all strategy of the RE vis-à-vis adoption of IT, and ensure that the IT Strategy aligns with the overall strategy of the RE towards accomplishment of its business objectives;
c) Be satisfied that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has well defined objectives and unambiguous responsibilities for each level in the organisation;
d) Ensure putting in place processes for assessing and managing IT risks, including cyber security risks;
e) Ensure that the budgetary allocations for the IT function (including for IT security) are commensurate with the RE's IT maturity, digital depth, threat environment and industry standards and are utilised in a manner intended for meeting the stated objectives; and
f) Have responsibility and oversight over the Business Continuity Planning and Disaster Recovery Management of the RE.

Senior Management

9. CEO of the RE shall have the overall responsibility and institute an effective oversight on the plan and execution of IT Strategy; put in place appropriate mechanism to ensure IT/ IS and their support infrastructure are functioning effectively and efficiently; cyber security posture of the RE is robust; and overall, IT contributes to productivity, effectiveness and efficiency in business operations.

10. REs shall establish an IT Steering Committee with representation at Senior Management level from IT, business functions for assisting the Board/ IT Strategy Committee in the implementation of the IT Policy and IT Strategy. The IT Steering Committee shall meet at least on quarterly basis. The responsibilities of IT Steering Committee, *inter alia,* shall be to:
    a) Assist the Board/ IT Strategy Committee in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs;
    b) Update Board/ IT Strategy Committee and CEO periodically on the activities of IT Steering Committee;
    c) Oversee the business continuity planning process including determining how it will manage and control identified risks as well as prioritise critical business

functions; putting in place a framework/ mechanism for effective Disaster Recovery Management;

d) Define IT project success measures and follow up progress on IT projects;
e) Ensure compliance with technology standards and guidelines; and
f) Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance.

Head of IT Function

11. REs shall appoint a sufficiently senior level, technically competent and experienced person in IT related aspects as Head of IT Operations[4]. The Head of IT Operations shall play a key role in decision-making involving the use of IT in the RE.

12. The Head of IT Operations shall establish an effective organisation to support IT operations in the RE and shall, *inter alia*, be responsible for the following:
    a) Ensuring implementation of IT Policy, IT Strategy and Vision of the RE.
    b) Putting in place documented IT Standard Operating Procedures.
    c) Ensuring that the execution of IT projects/ initiatives is aligned with the RE's IT Policy and IT Strategy.
    d) Implementing and managing suitable IT architecture that efficiently supports existing as well as future IT capabilities needed by the business.
    e) Putting in place an effective disaster recovery setup and business continuity strategy/ plan.
    f) As a first line of defence, ensuring effective assessment, evaluation and management of IT risk including the implementation of robust internal controls to (i) secure the RE's information/ IT assets (ii) comply with extant internal policies, regulatory and legal requirements on IT related aspects.
    g) Ensuring adherence to extant instructions[5] on Outsourcing of IT activities.

13. Requirements for trained resources with requisite skill sets for the IT function shall be understood and assessed appropriately by the Head of IT Operations. A periodic assessment of the training requirements for human resources shall be made to ensure that sufficient, competent and capable human resources are

[4] By whatever name called viz. Chief Technology Officer or Chief Information Officer, etc.
[5] Master Direction on Outsourcing of IT Services

available. REs shall have a documented training plan/ programme for periodic training/ awareness workshops for the members of its Board, Senior Management, CxOs, members of the IT Function and other employees on aspects pertaining to IT and Information Security. The plan shall be implemented and tracked for its effectiveness.

Chapter III

IT Infrastructure & Services Management

IT Services Management

14. A robust IT Service Management Framework shall be established for supporting IT systems and infrastructure of the RE, to ensure the operational resilience of the entire IT environment of the RE (including DR sites).

15. A Service Level Management (SLM) process shall be put in place to manage the IT operations while ensuring effective segregation of duties.

16. For seamless continuity of business operations, REs shall avoid using outdated and unsupported hardware or software and shall monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on ongoing basis. REs shall develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach EOS.

17. REs shall ensure clock/ time synchronisation between all its IT systems using appropriate protocols.

18. REs shall be guided by the following instructions for third-party arrangement in the Information Technology/ Cyber Security ecosystem that are either not considered as "outsourcing" of IT Services arrangement (for example - purchase of hardware, software) (or) not considered as "material" outsourcing of IT Services. In general, REs shall put in place appropriate vendor risk assessment and controls proportionate to the risk and materiality assessed and ensure inter alia to a) mitigate concentration risk including aspects pertaining to conflict of interest; b) mitigate risks associated with single point of failure; c) comply with applicable legal, regulatory requirements and standards to protect customer data; d) provide high availability; and e) manage supply chain risks effectively (as per applicability of the arrangement)[6].

[6] REs may consider applying the instructions provided in "Master Direction on Outsourcing of IT Services" to their non-material IT outsourcing also, if felt necessary, depending upon the risk perceived.

Capacity Management

19. Capacity management is a critical objective of IT Function and REs are required to proactively assess any capacity constraint based on past trend (peak usage), business activities (current as well as future plans) and address the issues effectively. Annual assessment of capacity vis-a-vis the expectations, with sufficient safety margin shall be carried out, and the same shall be reviewed by the Board/ Board level IT Strategy Committee.

20. REs shall ensure that IT systems and infrastructure are able to support business functions and ensure availability of all service delivery channels.

21. IT Capacity planning across all components, services, system resources, supporting infrastructure shall be consistent with the current business requirements and projected future needs as per the IT strategy of the RE.

Project Management

22. REs while adopting new/ emerging technologies, tools or revamping their existing ones in the technology stack, shall follow a standard enterprise architecture planning methodology/ framework. Such adoption including Artificial Intelligence, Automation, Application Programming Interfaces (APIs), new emerging technologies shall be commensurate with the risk appetite and align with overall Business/ IT strategy of the RE. This should facilitate optimal creation, use and/ or sharing of information by a business, in a way that it is secure and resilient. REs shall maintain enterprise data dictionary to enable the sharing of data among applications and systems and promote a common understanding of data among IT and business users.

23. A consistent and formally defined project management approach shall be applied to IT projects undertaken by the RE. The project management approach shall, *inter alia*, enable appropriate stakeholder participation for effective monitoring and management of project risks and progress.

24. Information on major IT projects that have a significant impact on the RE's risk profile and strategy shall be reported to the IT Strategy Committee. Such projects shall undergo appropriate strategic and cost/ reward analysis on a periodic basis.

25. REs shall ensure that source codes for all critical applications are received from the vendors or a software escrow agreement is in place with the vendors for ensuring continuity of services in case the vendor defaults or is unable to provide services. REs shall also ensure that product updates and programme fixes are also included in the escrow agreement. Where the code is not owned by the RE, then, in such cases, the RE shall obtain a certificate from the application developer stating that the application is free of known vulnerabilities, malwares and any covert channels in the code.

26. Any new IT application proposed to be introduced as a business product, along with its underlying information systems, shall be subjected to formal product approval and quality assurance process which shall, inter-alia, assess functionality, security, performance related aspects and compliance to relevant legal and regulatory prescriptions. While designing and implementing various applications/ systems, REs shall ensure high availability and fault tolerance requirements.

Change Management

27. REs shall put in place a 'Change Management' procedure for handling any changes in technology and processes to ensure that the changes in the IT systems are implemented and reviewed in a controlled manner and in a controlled environment.

28. Similarly, procedures to assess the effectiveness of integration and interoperability of complex IT processes shall be put in place. Patches as per their criticality shall be evaluated in a test environment before being pushed into live environment.

Data Migration Controls

29. REs shall have a documented data migration policy specifying a systematic process for data migration, ensuring data integrity, completeness and consistency. The policy shall, inter-alia, contain provisions pertaining to signoffs from business users/ application owners at each stage of migration, audit trails etc.

Outsourcing of IT Services

30. REs shall be guided by extant instructions[7] on Outsourcing of IT Services.

Audit Trails

31. Every IT application which can access or affect critical/ sensitive information, shall have audit trails/ logging capability with details like transaction id, date, time, originator id, authoriser id, actions undertaken by a given user id, etc. Other details like logging IP address of client machine, terminal identity or location shall also be available, wherever applicable.

32. The IT policy of the RE shall articulate the preservation period of such audit trails and logs, considering the regulatory and legal requirements.

33. The audit trails shall satisfy a RE's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes. Audit trails shall be secured to ensure the integrity of the information captured and preservation of evidence. REs shall put in place effective log management and retention framework that is comprised of tools to manage, collect and store system and application logs that would be required to facilitate incident investigation and analysis.

[7] Master Direction on Outsourcing of IT Services

Chapter– IV

IT Risk and Information Security

IT Risk Management

34. The risk management policy of the RE shall include IT related risks, including the Cyber Security related risks, and the Risk Management Committee of the Board shall periodically review and update the same at least on a yearly basis.

35. REs shall establish a robust IT Risk Management Framework covering the following aspects:
    a) Identification of the RE's IT assets and their security classification based on their criticality to the RE's operations;
    b) Objective and periodic assessment of the risks – internal and external – facing the RE's IT assets/ infrastructure, including an evaluation of their likelihood and impact;
    c) Implementation of comprehensive information security management function, internal controls and processes (including applicable insurance covers) to mitigate/ manage identified risks. The implemented controls and processes must be reviewed periodically on their efficacy in a risk environment characterised by change;
    d) Define roles and responsibilities of stakeholders (including third-party personnel) involved in risk management. Areas of possible role conflicts (where more than one stakeholder takes responsibility) and accountability gaps (where no stakeholder takes responsibility) must be specifically identified and eliminated/ managed;
    e) Identification of Crown Jewels[8] of the organisation and fortification the security environment of such systems; and
    f) Evaluation of systems so as to understand whether any or group of such systems need to be identified as 'Critical Information Infrastructure' in terms of extant instructions issued by appropriate authorities under the law. Evolve standard operating procedures in identifying and protecting such systems/ group of systems.

[8] "Crown Jewels" are information systems that are most critical to the accomplishment of an organisation's objectives.

IT Risk Metrics

36. REs shall define appropriate metrics for system performance, recovery and business resumption, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO), for each IT system/ service/ application.

37. REs shall implement appropriate scorecard/ metrics/ methodology to measure IT performance and IT maturity level.

Information Security Policy and Cyber Security Policy

38. The Board shall establish necessary organisational processes/ functions for information security and provide necessary resources. The Information Security Policy shall take into consideration, inter alia, aspects such as alignment with business objectives; the objectives, scope, ownership and responsibility for the Policy; information security organisational structure; information security roles and responsibilities; exceptions; knowledge and skill sets required; periodic training and continuous professional education; compliance review and penal measures for non-compliance of Policies. REs shall also put in place a Cyber Security Policy. Cyber Crisis Management Plan (CCMP) shall address the following aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment.

39. An Information Security Committee (ISC), under the oversight of the Risk Management Committee (RMC) of the Board, shall be formed for managing information security. The constitution of the ISC with Chief Information Security Officer (CISO), other representatives from business, IT functions, etc., shall be decided by the RMC. Major responsibilities of the ISC, inter alia, shall include:
    a) Facilitating development of information security policies, implementation of information security policies, standards and procedures to ensure that all identified information security risks are managed within the RE's risk appetite;
    b) Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving standards and procedures;
    c) Supporting the development and implementation of information security management programme;

d) Reviewing information/ cyber security incidents, various information security assessments, monitoring and mitigation activities across the RE;
e) Reviewing security awareness programmes;
f) Assessing new developments or issues relating to cyber/ information security; and
g) Reporting to the Board/ Board level Committee on information security activities.

40. A sufficiently senior level executive shall be designated as the Chief Information Security Officer (CISO). The CISO shall not have any direct reporting relationship with the Head of IT Operations and shall not be given any business targets. REs shall ensure the following:
    a) The CISO has the requisite technical background and expertise.
    b) She/He is appointed for a reasonable minimum term.
    c) The CISO's Office is adequately staffed with people having necessary technical expertise, commensurate with the business volume, extent of technology adoption and complexity.
    d) The budget for the information/ cyber security, CISO's Office is determined keeping in view the current/ emerging threat landscape.

41. REs shall ensure that the roles and responsibilities of the CISO are clearly defined and documented covering, at a minimum, the following points:
    a) The CISO shall be responsible for driving and ensuring compliance to the extant regulatory instructions on information/ cyber security.
    b) The CISO shall be responsible for articulating and enforcing the policies that a RE uses to protect its information assets apart from coordinating information/ cyber security related issues/ implementation within the RE as well as with relevant external agencies.
    c) The CISO shall be an invitee to the IT Strategy Committee and IT Steering Committee.
    d) The CISO shall ensure that current and emerging cyber threats to the financial sector and the RE's preparedness in these aspects are discussed in ISC and other related Committees.

e) The CISO's Office, in co-ordination with Head of IT Operations (as required), shall manage and monitor Security Operations Centre (SOC) and drive cyber security related projects.

f) The CISO shall coordinate the activities pertaining to Cyber Security Incident Response Team (CSIRT) within the RE.

g) The CISO shall develop cyber security KRIs and KPIs.

h) The CISO shall have a robust working relationship with Chief Risk Officer (CRO) to enable a holistic risk management approach. To this effect, the CRO may be invited to ISC meetings. CISO may be a member of (or invited to) Committees on Operational Risk where IT/ Information Security risk is also discussed.

i) CISO shall place a separate review of cyber security risks/ arrangements/ preparedness of the RE before the Board/ Board level Committee on a quarterly basis.

Information Security Management

42. REs shall define and implement necessary systems, procedures and controls to ensure secure storage/ transmission/ processing of data/ information.

43. REs may consider implementing security standards/ IT control frameworks (such as ISO 27001) for their critical functions.

44. REs shall ensure that the privacy-related safeguards, as required by laws and regulations, are built into their information management framework.

45. The risk assessment for each information asset within the RE's scope shall be guided by appropriate security standards/ IT control frameworks. It shall entail identifying the threat/ vulnerability combinations that have a likelihood of impacting the confidentiality, integrity and availability of that information asset (including stored and processed data/ information) – from a business, compliance and/ or contractual perspective.

46. RE shall ensure that all staff members and service providers comply with the extant information security and/ or acceptable-use policies as applicable to them.

47. REs shall review their security infrastructure and security policies at least annually, factoring in their own experiences and emerging threats and risks. REs shall take steps to adequately tackle cyber-attacks including phishing, spoofing attacks and mitigate their adverse effects.

48. The key length (for symmetric/asymmetric encryption, hashing), algorithms (for encryption, signing, exchange of keys, creation of message digest, random number/ key generators), cipher suites and applicable protocols used in transmission channels, processing of data, authentication purpose, shall be strong, adopting internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls are compliant with extant laws and regulatory instructions.

49. Data transfer from one process to another or from one application to another, particularly in respect of critical or financial applications, shall not have any manual intervention in order to prevent any unauthorised modification. The process must be automated and properly integrated through "*Straight Through Processing*" methodology with an appropriate authentication mechanism and audit trails.

Physical and Environmental Controls

50. REs shall implement suitable physical and environmental controls to prevent impairment of data through physical access and damage or destruction to physical infrastructure/ facilities (DC and DR[9] sites).

51. RE's DC and DR sites should be geographically well separated so that both the sites are not affected by a similar threat associated to their location. REs shall ensure that their DC and DR sites are adequately monitored through CCTV cameras and recordings thereof are reviewed on an ongoing basis.

[9] DC refers to primary data centre for a given application/ system and DR its Disaster Recovery site/ alternate site.

Access Controls

52. Access to information assets shall be allowed only where a valid business need exists. There shall be documented standards/ procedures, which are approved by the competent authority and kept up to date, for administering need-based access to an IT system.

53. Personnel with elevated system access entitlements shall be closely supervised with all their systems activities logged and periodically reviewed. REs shall adopt multi-factor authentication for privileged users.

Controls on Teleworking

54. The controls to be put in place in a teleworking environment (a non-exhaustive list) are:
    a) Ensure that the systems used and the remote access[10] from Alternate Work Location (AWL) to the environment hosting RE's information assets are secure (using necessary encryption);
    b) Put in place multi-factor authentication for enterprise access (logical) to critical systems;
    c) Mechanism to identify all remote-access devices attached/ connected to the RE's systems shall be put in place.
    d) Teleworking, where remote access to the RE's systems is not provided shall be secured appropriately depending upon the sensitivity of the data/ information shared/ handled.

VA/PT Assessments

55. REs shall periodically conduct Vulnerability Assessment/ Penetration Testing (VA/ PT) of the IT assets (applications, systems and infrastructure) throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.) by appropriately trained and independent information security experts/ auditors. For critical IT assets and/ or those in the DMZ (De-Militarized Zone), VA shall be conducted at least once in every six months and PT at least once in 12 months.

[10] The remote access methods most commonly used by teleworkers are divided into four categories based on their high-level architectures: tunnelling, portals, direct application access, and remote desktop access. Define one or more means of secure access from remote locations, which best fits the enterprise architecture, scale of operations and the RE's requirement.

VA/ PT for (a) all other IT assets; (b) when any new IT Infrastructure or application is introduced (or) existing application has undergone any major change; shall be conducted, basis their criticality and inherent risks as defined by the RE.

56. In the post implementation (of IT project/ system upgrade, etc.) scenario, the VA/ PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, REs shall ensure that the version and configuration of the test environment resembles the production environment. Any deviation should be documented and approved by the ISC.

57. REs may also run automated VA scanning tools to automatically scan all systems on the network that are critical, public-facing or store customer sensitive data on a continuous/ more frequent basis.

58. REs shall ensure to fix the identified vulnerabilities and associated risks in a time-bound manner by undertaking requisite corrective measures and ensure that the compliance is sustained to avoid recurrence of known vulnerabilities.

59. REs shall ensure that all vulnerability scanning is performed in authenticated mode.

60. REs shall have a mechanism in place to carry out the PTs in a controlled manner within the scoped IT system components/ applications for any known as well as unknown vulnerability which may exist before the PT exploits.

61. REs shall put in place a documented approach for conduct of VA/ PT covering the scope, coverage, vulnerability scoring mechanism (e.g., Common Vulnerability Scoring System) and all other aspects. This may also apply to the RE's infrastructure/ application hosted in a cloud environment.

Incident Response and Recovery Management

62. The incident response and recovery management policy shall address the classification and assessment of incidents; include a clear communication strategy and plan to manage incidents, contain exposures and achieve timely recovery.

63. Any event or the threat of such an event adversely impacting the confidentiality, integrity and/ or availability of (i) information assets of the RE and/ or (ii) the physical infrastructure and/ or environment hosting the information assets of the RE shall be considered as an incident.

64. REs shall take measures to mitigate the adverse impact of such incidents on business operations.

65. REs shall analyse the incidents (including through forensic analysis, if necessary) for their severity, impact and root cause.

66. REs shall have written incident response and recovery procedures including identification of key roles of staff/ outsourced staff handling such incidents.

67. REs shall have clear communication plans for escalation and reporting the incidents to the Board and Senior Management as well as to customers, as required. REs shall pro-actively notify CERT-In and RBI regarding cyber security incidents, as per regulatory requirements. REs are also encouraged to report the incidents to Indian Banks – Centre for Analysis of Risks and Threats (IB-CART) set up by IDRBT.

68. REs shall establish processes to improve incident response and recovery activities and capabilities through lessons learnt from past incidents as well as from the conduct of tests and drills. REs, *inter alia*, shall ensure effectiveness of crisis communication plan/ process by conduct of periodic drills/ testing with stakeholders (including service providers).

69. RE's BCP/ DR capabilities shall be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations (including security controls) post cyber-attacks/ other incidents.

Chapter V

Business Continuity and Disaster Recovery Management

Business Continuity Plan

70. RE's Board shall have ultimate responsibility and oversight over the business continuity of a RE. The BCP/ policy shall adopt best practices based on international standards (e.g., ISO 22301), to guide its actions (including defining the responsibilities) in reducing the likelihood or impact of the disruptive incidents and maintaining business continuity. The policy shall be updated based on major developments/ risk assessment.

71. REs shall ensure business continuity even in the event of unforeseen disruptive incidents. REs shall undertake a business impact analysis/ assessment of the likelihood of an adverse event and assess its impact on the RE's information assets and the associated business operations.

72. REs shall regularly test the BCP under different scenarios for all possible types of contingencies, to ensure that it is up-to-date and effective. Testing of BCP shall include all relevant aspects and constituents of the RE i.e. People, Processes and Resources (including Technology).

Disaster Recovery Management

73. Periodicity of DR drills for critical systems shall be at least on a half-yearly basis and for all other systems at least on a yearly basis. Any major issues observed during the drill shall be resolved and tested again, to ensure successful conduct of drill before the next cycle. The DR testing shall involve switching over to the DR/ alternate site and thus using it as the primary site for sufficiently longer period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.

74. REs shall backup data and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved along with securing it from unauthorised access.

75. REs shall ensure that, DR architecture and procedures are robust meeting the defined RTO and RPO for any recovery operations in case of contingency.

76. In a scenario of non-zero RPO, REs shall have a documented methodology for reconciliation of data, while resuming operations from the alternate location.

77. REs shall ensure that the configurations of servers, network devices, other products and deployed security patches at the DC and DR[11] are identical.

78. REs shall ensure BCP and DR capabilities in critical interconnected systems and networks including those of vendors and partners. REs shall ensure demonstrated readiness through collaborative & co-ordinated resilience testing that meets the RE's RTO.

[11] DC refers to primary data centre for a given application/ system and DR its Disaster Recovery site/ alternate site.

Chapter VI
Information Systems (IS) Audit

Information Systems (IS) Audit

79. The Audit Committee of the Board (ACB)/ Local Management Committee ((LMC) in case of foreign banks) shall be responsible for exercising oversight of IS Audit of the REs.

80. REs shall have an IS Audit Policy. The IS Audit Policy shall contain a clear description of its mandate, purpose, authority, audit universe, periodicity of audit etc. The policy shall be approved by the ACB/ LMC and reviewed at least annually.

81. The ACB/ LMC shall review critical issues highlighted related to IT/ information security/ cyber security and provide appropriate direction and guidance to the RE's Management.

82. REs shall have a separate IS Audit function within the Internal Audit function. Where the RE uses external resources for conducting IS audit in areas where skills are lacking within the RE, the responsibility and accountability for such external IS audits would continue to remain with the competent authority within Internal Audit function. The overall ownership and responsibility of the IS Audit including the audit planning process, risk assessment and follow up of compliance shall remain within the Internal audit function.

83. IS Auditors shall act independently of the RE's management. IS Auditors shall be professionally competent, having the skills, knowledge, training and relevant experience to conduct IS audit.

84. REs shall carry out IS Audit planning by adopting a risk-based audit approach in compliance with extant regulatory instructions on Risk-based Internal Audit.

85. REs may consider, wherever possible, a continuous auditing approach for critical systems, performing control and risk assessments on a more frequent basis.

86. REs may have standardised checklist, scoping document as reference material for conducting IS audits. Such a checklist may be updated on an ongoing basis to align with extant IT practices, regulations, systems deployed, vulnerabilities and threat landscape.

87. The IS audit reports shall be placed before the Senior Management, ACB and the compliance shall be ensured within the time frame as outlined in the audit policy of the RE.

CHAPTER – VII

REPEAL AND OTHER PROVISIONS

88. With the coming into effect of these Directions, the instructions/ guidelines contained in the following circulars issued by the Reserve Bank stand **repealed**. **All the repealed circulars are deemed to have been in force prior to the coming into effect of these Directions.**

(i) DBS.CO.ITC.BC.10/31.09.001/97-98 dated February 4, 1998 on Risks and Control in Computer and Telecommunication Systems

(ii) DBS.CO.OSMOS.BC/11/33.01.029/2003-04 dated April 30, 2004 on Information System Audit - A Review of Policies and Practices

(iii) DBS.CO.IS.Audit.No.19/31.02.03/2004-05 dated April 15, 2005 on Operational Risk Management - Business Continuity Planning

(iv) DBS.CO.IS.Audit.No.4/31.02.03/2005-06 dated February 16, 2006 on Business Continuity / Disaster Recovery Planning

(v) DBS.CO.IS.Audit.BC.No.3/31.02.03/2005-06 dated February 16, 2006 on Phishing Attacks

(vi) DIT.CO.801/07.71.032/201-11 dated September 29, 2010 on Business Continuity Plan (BCP), Disaster Recovery (DR) drill and Vulnerability Assessment-Penetration Testing (VAPT)

(vii) DIT.CO(Policy)2036/07.71.032/2011-12 dated March 2, 2012 on Business Continuity Plan (BCP) and Disaster Recovery (DR); Vulnerability Assessment-Penetration Testing(VAPT)

(viii) DIT.CO.(Policy).No.674/09.63.025/2013-14 dated August 30, 2013 on Sharing of Information Technology Resources by Banks – Guidelines

(ix) DIT.CO(Policy)No.2636/09.63.025/2012-13 dated June 26, 2013 on Business Continuity Planning (BCP), Vulnerability Assessment and Penetration Tests (VAPT) and Information Security

(x) DIT CO No.1857/07.71.099/2013-14 dated February 26, 2014 on Security Incident Tracking Platform - Reporting thereon

(xi) DBS (CO). CSITE/9094/31.01.15/2016-17 dated May 23, 2017 on Risk Governance Framework-Role of Chief Information Security Officer (CISO)

The following Master Direction is **repealed only for NBFC-Top, Upper and Middle Layer**.

(xii) DNBS.PPD.No.04/66.15.001/2016-17 dated June 08, 2017 on Master Direction - Information Technology Framework for the NBFC Sector

The following circulars are **consolidated**[12], while issuing these Directions:

(xiii) DBS.CO.OSMOS.BC.8/33.01.022/2002-2003 dated December 19, 2002 on Standardised Checklists for Conducting Computer Audit - Report of the Committee on Computer Audit

(xiv) DBS.CO.ITC.BC.No. 6 /31.02.008/2010-11 dated April 29, 2011 on Working Group on Information Security, Electronic Banking, Technology Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds- Implementation of recommendations.

****

[12] For compliance purpose, it is sufficient to adhere to this Master Direction by the REs in lieu of the circulars and the reports referred therein.

Acronyms

ACB	Audit Committee of the Board of Directors
API	Application Programming Interface
AWL	Alternate Work Location
BCP	Business Continuity Plan
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CCTV	Closed-Circuit Television
CERT-In	Indian Computer Emergency Response Team
CRO	Chief Risk Officer
CSIRT	Cyber Security Incident Response Team
CTO	Chief Technology Officer
CVSS	Common Vulnerability Scoring System
DMZ	De-Militarized Zone
DC	Data Centre
DR	Disaster Recovery
EOS	End of Support
IB-CART	Indian Banks – Centre for Analysis of Risks and Threats
IDRBT	Institute for Development and Research in Banking Technology
IP	Internet Protocol
ISC	Information Security Committee
IS	Information Systems
ISO	International Organization for Standardization
IT	Information Technology
ITSC	IT Strategy Committee
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LMC	Local Management Committee
PT	Penetration Testing
RBI	Reserve Bank of India

RE	Regulated Entity
RMC	Risk Management Committee
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SOC	Security Operation Center
VA	Vulnerability Assessment